

10/031681

TRANSMITTAL LETTER
(General Patent Pending)

Docket No.
09669/019001

In Re Application Of: Robert LEYDIER

531 Rec'd PCT/F

22 JAN 2002

Serial No.

Filing Date

Examiner

Group Art Unit

Title: MICRO-CONTROLLER PROTECTED AGAINST CURRENT ATTACKS

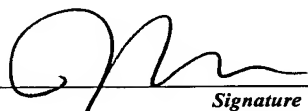
TO THE COMMISSIONER OF PATENTS AND TRADEMARKS:

Transmitted herewith is:

Translation of Article 34 Amendments (5 pages)

in the above identified application.

- ☒ No additional fee is required.
☐ A check in the amount of _____ is attached.
☒ The Commissioner is hereby authorized to charge and credit Deposit Account No. 50-0591
as described below. A duplicate copy of this sheet is enclosed.
- ☐ Charge the amount of _____
☒ Credit any overpayment.
☒ Charge any additional fee required.


Signature

Dated:

1/22/02

Jonathan P. Osha, Reg. No. 33,986
ROSENTHAL & OSHA L.L.P.
1 Houston Center, Suite 2800
1221 McKinney Avenue
Houston, Texas 77010

Telephone: 713/228-8600
Facsimile: 713/228-8778

CC:

I certify that this document and fee is being deposited
on _____ with the U.S. Postal Service as
first class mail under 37 C.F.R. 1.8 and is addressed to the
Commissioner of Patents and Trademarks, Washington,
D.C. 20231.

Signature of Person Mailing Correspondence

Typed or Printed Name of Person Mailing Correspondence

10/031681

CERTIFICATE OF MAILING BY "EXPRESS MAIL" (37 CFR 1.10)

Applicant(s): Robert LEYDIER

22 JAN 2002

09669/019001

Serial No.

Filing Date

Examiner

Group Art Unit

Invention: MICRO-CONTROLLER PROTECTED AGAINST CURRENT ATTACKS

I hereby certify that this Article 34 Amendments

(Identify type of correspondence)

is being deposited with the United States Postal Service "Express Mail Post Office to Addressee" service under
37 CFR 1.10 in an envelope addressed to: The Commissioner of Patents and Trademarks, Washington, D.C.

20231-0001 on 22 January 2002

(Date)

Toni A. Hill

(Typed or Printed Name of Person Mailing Correspondence)


(Signature of Person Mailing Correspondence)EV049244445US

("Express Mail" Mailing Label Number)

Note: Each paper must have its own certificate of mailing.

noise with considerable random or incorrect information while the instructions are being executed by the microcontroller.

However, these methods have numerous disadvantages. The program execution time is long. Considerable memory space is required.

5 Lastly, the confidential data is not protected against an in-depth analysis carried out by the defrauders since the electrical signal, which results from the execution of the instructions, is still present.

Another method, described in the French patent application No. 98 01305, and not made public on the priority date of this request,

10 suggests filtering the current with a low-pass filter cell. This method simply attenuates the electrical signatures and by analysing them in detail, certain confidential data can still be accessed.

The patent US 4 932 053 concerns the security of the confidential information contained in an integrated circuit. In a certain number of

15 applications concerning integrated circuits and more especially in smartcard type applications, unauthorised persons must be denied access to some of the confidential data contained in the memory of the circuit. To prevent the defrauder from examining the current consumption at the ends of the integrated circuit during a read or write

20 operation in the memory, a protection circuit is used. This protection circuit is used to activate the simulation, according to a pseudo-random sequence generated by a generator, of current consumption values identical to those of the true memory cells.

Lastly, note that the patent US 4 827451 concerns the field of

25 memories built in the form of a matrix of memory cells. The said cells, which can be accessed in lines and columns, are connected to read and write circuits which are used to program them in two states - "1" or "0" according to the input data - and read the state so programmed. The memory cells are the type which requires a programming current to be

30 programmed to "1" and which requires no current when programming to "0". The said security circuit consists of a simulation circuit activated

during a programming to "0" to supply a current identical to that supplied by a memory cell during a programming to "1".

5 In view of the above, a technical problem which the invention proposes to solve is to secure a portable object of type smartcard, including:

- a microcontroller including an efficient part to carry out data processing;
 - a contact stud to supply the said microcontroller with current;
 - 10 - a data input and/or output contact stud;
 - confidential data,
- against current attacks.

To achieve this, the invention proposes a portable object defined according to claim 1 and a microcontroller defined according to claim 7.

microcontroller in the state of the art technology (signature A) then for a microcontroller secured according to the invention (signature B);

- 5 - figure 12 is a wiring diagram of a special mode of realisation of a microcontroller according to the invention; and
- figure 13 shows the variations of signals S_1 , S_2 and S_3 against time, for a microcontroller corresponding to the mode of realisation of figure 12.

10 In the mode of realisation shown on figures 1, 2 and 3, a portable object according to the invention takes the form of a roughly rectangular thin card 1 including a body 2 integrated to an electronic module 3.

 The body 2 of the card consists, for example, of five plastic laminated sheets 20, 21, 22, 23 and 24 and includes a cavity 25 to
15 incorporate the module 3.

 Module 3 includes a microcontroller 30 whose contact studs 300 are electrically connected, via conducting wires 31, to contact pads 32 flush with the surface of the card body 2. These contact pads 32 rest on a thickness 33 of an epoxy glass type dielectric. The assembly
20 microcontroller 30 and conducting wires 31 is coated with a protective resin 34.

 In the mode of realisation shown on figure 4, the microcontroller 30 takes the form of a right parallelepiped of thickness about 180 μm and area about 10 mm^2 .

25 This microcontroller 30 includes a main layer 301 of silicon whose active face, which includes a circuit and supports the contact studs 300,